SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR CONDUCTING A SECURE TRANSACTION VIA A NETWORK

ABSTRACT

A system, method and computer program product for conducting a secure transaction via a network is disclosed. Coupled to a network are a first site and a terminal for permitting a user to perform a first portion of a transaction at the first site via the network. A second site is also coupled to the network for performing a second portion of the transaction which requires the use of personal data of the user. The second site is contacted by the first site via the network to perform the second portion of the transaction. In response, the second site transmits a certificate for verifying the identity of the second site to the terminal via the network. After the terminal authenticates the certificate, the second site then transmits a request for the personal data to the terminal via the network. A secure device associated with the user is coupled to the terminal. The secure device contains an encrypted version of the personal data and a first key for decrypting the encrypted personal data. In response to the request for personal data, the secure device provides the terminal with the encrypted personal data and the first key. The terminal decrypts the encrypted personal data using the first key, re-encrypts the decrypted personal data with a second key, and then transmits the re-encrypted personal data to the second site via the network.